Process Monitoring Tool (ProcMon)

Description:

It is Simple Process monitoring Tool which can be used to retrieve information about current running Process on system. Apart from that it also help us to view the thread ID's, DLL (dynamic link library) files associated with that process. The tool is menu based therefore it is easy for user. It is also helpful to display memory uses of given process. Hardware configuration of current system can be also included which shows OEM ID, number of processors, processor type etc.

This tool also maintains a log file whenever user want to save current information about process then he can create log file by simply providing "log" command to the application. The log file is created in d drive with name of date and time when log file created the log file can be also be readed using "readlog" command.

Technology:

- Windows Programming using c++(WIN32 SDK)
- Visual Studio 2012 (IDE)

Platform required:

- Windows NT Platform

User Interface:

- CLI (Command Line Interface)

Hardware Requirement:

- Intel 32bit Processor
- Hard disk partitioned with volume label D:\

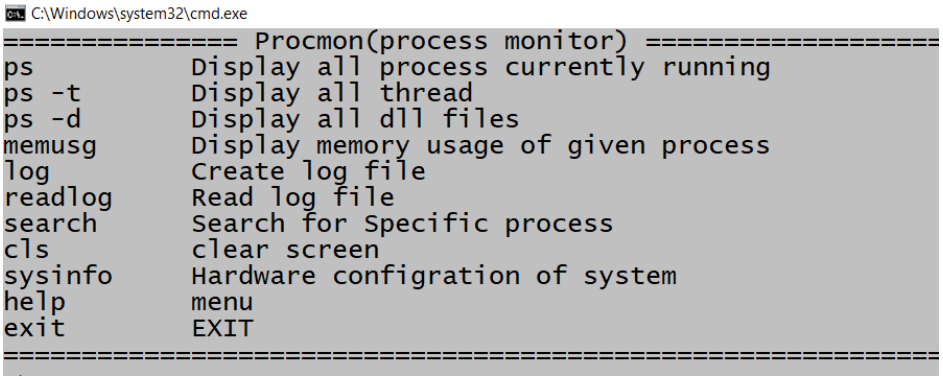
Data Structure used:

- Multi-dimensional arrays
  In this project we have used multi-dimensional array to store process id, thread Id's, modules and display it.

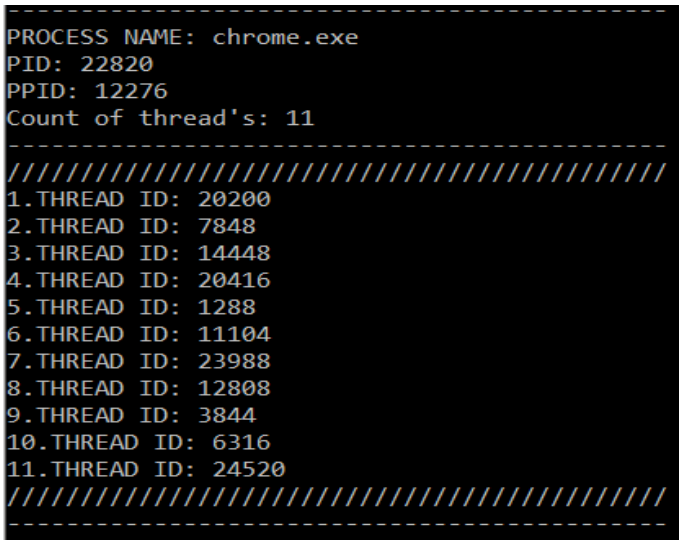
- Files
  Files is used to Store information about process id, thread Id's in log.

Features:

1. Menu



2. Processes Information Dialog



Question's:

1. Explain flow and Working of your project?

   It is a command based application so it takes text from user
   And shows output accordingly.
   For ex. When user type "ps" then it will shows all the process
   And if user types "ps –t" it will show process and its associated threads.
   When user press "ps" then internally it takes snapshot of processes
   Using CreateToolhelp32snapshot () function which is provided in TLhelp32.h and iterate through all process and display its information.

2. What is mean by Process?

   A process or running process refers to instruction currently being processed by the computer processer.
   A computer program is passive collection of instructions. A process is actual execution of those instructions.

3. What is difference between Process & Thread?

Processes	Threads
Processes is any program in execution.	Threads means segment of process.
More time to terminate.	Less time to terminate.
Consumes more resources.	Consumes less resources.
Completely isolated and do not share memory.	Shares memory with each other.
Process can exist individually.	A thread cannot have individual existence.
If process dies then all threads die including threads.	At time of expiration of thread its associated stack could be recovered as every threads has its own stack.

4. What is the use of ProcMon tool?

   Procmon can be used by system administrator to monitor process Running on system and one of the most use of this tool is that we can create log file which maintains all records.

5. What is mean by Windows API?

   Windows API (WinAPI) is core set application programming interfaces (API's) available in Microsoft windows operating system. Pretty much everything that a windows program does involves calling various API functions.

6. Explain the concept of Dynamic Link Libraries?

   Dynamic Link Libraries are like EXE's but they are not directly executable. DLL are Microsoft implementations of shared libraries (.so) in Linux/Unix.
   A DLL contains functions, classes, variables, UI's and resources (such as images and icons) that an EXE or other DLL uses.
   In Windows there are 2 types of libraries one is static library (.lib) and dynamic library (.dll) static libraries links with EXE at compile time while dynamic libraries linked with EXE's at run-time.

7. How you will fetch information of running processes in your project?

   As mentioned earlier when user press "ps" then internally it takes snapshot of processes
   Using CreateToolhelp32snapshot () function which is provided in TLhelp32.h and iterate through all process and display its information.

8. What are the features provided by the Procmon tool?

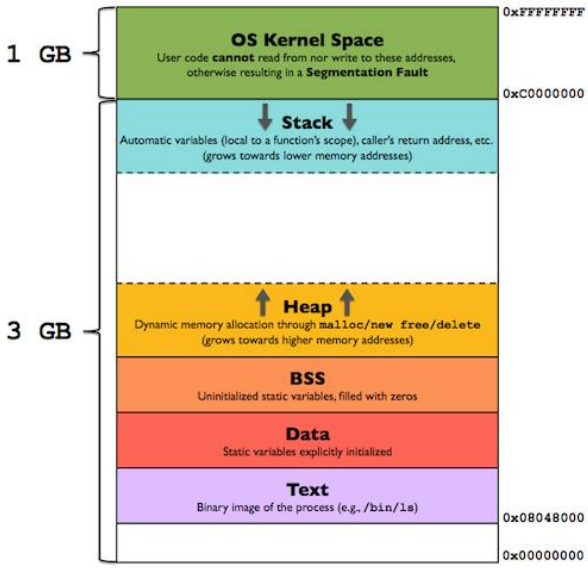
   - Process information.
   - Thread ID's associated with process.
   - Modules associated with process.
   - Memory usage of process.
   - Kill process.
   - Log file creation.
   - Searching for process.
   - Hardware configuration.

9. Explain data structures used by operating system to manage all running process?

   Just like any other software operating system needs data structure to work.
   Process Control Block (PCB) or Task Control Block is data structure in operating system kernel containing information needed to manage the scheduling of particular process.
   The details of the structures are system dependent, we can identify Some very common parts, and classify them into three main categories

   - Process identification data
   - Process state data
   - Process control data

10. Explain Memory layout of Process?



   Stack Section: This section contains local variable function and returns address. As in the diagram show stack and heap grow in opposite direction which is obvious if both grow in the same direction then they may overlap so it is good if they grow in opposite direction.

   Heap Section: This Section is used to provide dynamic memory whenever memory is required by the program during runtime it is provided form heap section.

BSS Segment: it is also refers to uninitialized data segment data in this segment is initialized by OS kernel to arithmetic zero before program start executing.

Data Section: the data segment is shorthand for initialized data segment this portion virtual address space of a program contains the global variables and static local variables.

Text: this segment also known as code segment is the section of memory which contains executable instructions of a program

11. How you maintain log file in your project?

The log of file of current process information is created when user gives command "log" after that it will again take snapshot of processes. And iterate through processes and associated thread ids At the time of iterating it will store the information in two dimensional arrays since process names are string literals and thread id are integers we have used array of char pointers to store process name and array of integers to store thread id.
After that this array will written in a file in d drive with name of current data, time, and min.

12. What is difference between static linking and dynamic linking?

In Windows there are 2 types of libraries one is static library (.lib) and dynamic library (.dll) static libraries links with EXE at compile time while dynamic libraries linked with EXE's at run-time.

13. Can we fetch information of specific information of process using your project?

YES, for this you have press "search YOUR PROCESS NAME" it give you information about process

14. Which Windows API are used in your project?

We have used win32API of windows in which we have used Tool Help Library which contains functions like CreateToolhelp32snapshot () for taking snapshot of processes.
And we have also used psapi (Process Status API) to retrieve information about processes, threads, modules.

15. What are the resources that you refer during development of this Project?

[1] MSDN (Microsoft developer network)

[2] Windows Internals, Part 1, 6th Edition by Mark E. Russinovich, David A. Solomon, Alex Ionesc.

[3] Sysinternals Suit Guide by Mark E. Russinovich

16. Which difficulty the you faced in this project?

I have found some difficulties while developing this project but I am accepted that difficulties as challenge.
The first one is that finding resources because as beginner it is important to take right path towards development. But after some research I have found two book which mentioned in above question which are really helpful to me.
After that I get really confused with arrays, file handling for creating log files, structures although I have learnt all these concept prior of developing this project but using these concepts actually in live Project is challenging.
Meanwhile I have accepted all difficulties as challenge and finished my project.

17. Is there any chance of improvement in your project?

YES, improvements needs in log file which currently DLL modules Are not get Written in log file.
And we can me this tool a GUI based which quite helpful to users.

18. Can we use this project one different platforms?

Currently this project is only developed for windows platform.

19. What are the names of Windows primary DLL?

ADVAPI32.DLL- one of the primary windows subsystem DLLs providing access to APIs for system shutdown, restart, registry access and user account management.

GD32.DLL- Provides Graphical Functions.

HAL32.DLL- the Hardware Abstraction Layer (HAL) DLL which allows which allows windows to run on different hardware platform.

KERNEL32.DLL- Provides Kernel Functions.

NTDLL.DLL- Exposes many of the native windows API functions to user mode application.

NTOSKRNL.EXE- Kernel image for windows os.

20. Explain Process scheduling mechanism in windows?

Process scheduler is component of the operating system which responsible for deciding whether the currently running process should continue running and if not, which process should run next.

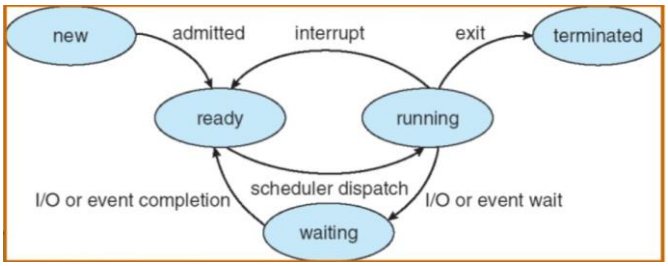


Fig. CPU Scheduler

Windows Scheduling:

Windows NT based operating system use multilevel feedback queue. 32 priority levels are defined

- Give preference to short jobs
- Give preferences to I/O bound Processes
- Quickly establish the nature of a process and schedule the process accordingly

All processes receive a priority boost after a wait event, but processes that have experienced a keyboard I/O wait get larger boost than those that have experienced a disk wait.

Windows XP schedules threads using priority based, pre-emptive scheduler with a flexible system of priority levels that includes round robin scheduling within each levels.
The scheduler ensures that highest priority thread will always run
The portion of windows kernel that handle scheduling is called dispatcher.